REMARKS

Claims 1-16 and 23-29 are pending. Claims 17-22 were previously cancelled. Claims 9-13, 25, 26 and 30-36 were previously withdrawn pursuant to the Examiner's restriction requirement, and are hereby cancelled without prejudice to Applicants continuing their prosecution in the copending and commonly owned divisional application No. 11/426,821.

The Examiner's allowance of claims 1-8, 14, 23-24, 27-28, and 37-39 and indication that claim 29 contains allowable subject matter are noted with appreciation.

Reconsideration is respectfully requested in light of the foregoing amendments and the following. Applicant also respectfully requests that the finality of the Action be withdrawn.

I. Claim Rejections Based on Hsu

In the Action, the Examiner rejected claims 15, 16 and 36 under 35 U.S.C. § 102(e) based on Hsu (EP 0924657). We respectfully traverse.

HSU

Hsu refers to a closed system designed for the singular purpose of verifying the identity of a person seeking access to a remote protected property, where the person seeking access to the remote property has been pre-registered with that remote property based on a code word generated from, but which is not itself, a biometric attribute. Hsu discloses at column 5, lines 48-50, "A person seeking entry to the door 10 carries a small handheld device, which may be integrated into a cellular telephone...." The single integrated circuit of the present invention as defined in claim 15 is not, in and of itself, a "small handheld device," but rather is a unique integrated semiconductor circuit (or chip) that must reside within a separate host handheld device.

Hsu teaches a fingerprint sensor 16 attached to or integrated with a device 14. To first initialize device 14, a full resolution image of the user's fingerprint is captured by sensor 16 and transferred to RISC processor 26. RISC processor 26 enhances the image creating a binarized/trinarized replica and then parses the processed image into small multiple "image patches" – each reference image patch containing what is believed to be a significant fingerprint feature (see U.S. Pat. No. 6,134,340, Figure 4, which is incorporated by reference at Hsu col. 7, line 39-42). The reference image patches are then stored by the registration program in an *unsecured* memory 32. On subsequent use of device 14, a captured fingerprint image is compared to the numerous reference image patches by use of image-to-image correlation techniques to determine a match. If a match is determined positive, a Cyclic Redundancy Code[1] generator 30 is then executed on the stored reference image patches – not the newly captured image – to create a 128 bit binary (CRC) number (see Hsu col. 7, lines 50-56). The binary CRC number is then encrypted and readied for transmission.

Applicant notes the following points about Hsu which are relevant to why Hsu does not teach or suggest what is called for in Applicant's claim 15:

- Device 14 contains no secure memory area where user-specific information may be safely stored.

[1] A Cyclic Redundancy Check (CRC) is a type of hash function used to produce a checksum – a small, fixed number of bits – against a block of data, such as a packet of network traffic or a block of a computer file. The checksum is used to detect errors after transmission or storage. Classically, a CRC is computed and appended to the data used to create the CRC number before transmission or storage. Then, the CRC can be verified afterwards by the recipient to confirm that no changes occurred on transit or on recall from storage. CRCs are popular because they are simple to implement in binary hardware, are easy to analyze mathematically, and are particularly good at detecting common errors caused by noise in transmission channels.

- Device 14 stores multiple small binary/trinary reference *image patches* with each image patch containing a single fingerprint feature – not an indicia that represents the algorithmic entirety of a fingerprint (a biometric attribute).
- Neither the captured fingerprint image nor the image patches are ever transmitted to a door 10 or any other remote location for subsequent use, verification, or viewing.
- Device 14 transmits only a binary CRC (or checksum) number that is derived from the reference image patches – it does not transmit the image patches themselves or the originally captured image.
- As implemented by Hsu, the CRC number is not appended to the underlying message string or data used to produce the CRC number, as would normally be the case.
- A CRC number cannot be used to reconstruct the reference image patches or to search other fingerprint databases for an identifying feature match.

Hsu states: "Before using the device 14 for access to a particular door 10 for the first time, the user 12 must first "register" at the door. (Hsu col. 8, lines 4-18.) The registration process is one in which an administrator of the door stores the user's name (or account number, or other identifying information), in association with a public encryption key to be used in the user's device 14, and the user's CRC as derived from the user's reference fingerprint image patches. If the door 10 provides access to a financial institution, for example, the user will register by bringing his or her device 14 to the institution, and transmitting the generated CRC from the device to the door receiver 15. In the registration mode, the door receiver 15 will store the user's CRC in association with the user's name or other identifying information." Applicant notes that according to Hsu:

- Door 10 does not use, store, or verify fingerprint features as a prerequisite to access.
- The user and his or her device 14 must be physically present to register at each door 10 where they may require access.
- Only the binary CRC number is transmitted from device 14 to door receiver 15.
- Device 14 does not contain user financial information nor is door 10 capable of receiving or acting upon user financial data.

CLAIM 15

In rejecting claim 15, the Examiner contends that:

> "Hsu discloses a portable wireless communications device (cellular phone 14'...) comprising a multi-function integrated semiconductor device having integrated in a single integrated circuit (inherently included in cellular phone 14') a personal database secure to all but a specified user (a reference fingerprint image stored in the device 14')" (Action at 3-4).

We respectfully disagree.

First and foremost, Hsu does not disclose or suggest either (1) a personal database secure to all but a specified user or (2) granting the user access to the secure personal database only on biometric verification. In point of fact Hsu does not teach or suggest a secure memory area of any type. Rather, Hsu teaches away from what is called for in Claim 15 in teaching to use only a separate, *unsecure* memory location 32 in which multiple reference image segments or "patches" are stored. See U.S. Patent 6,134,340, which is incorporated by reference (Hsu, col. 7, lines 38-42). Significantly, in the Hsu structure, anyone can access, erase and replace the image patches contained in device 14 simply by selecting the registration mode of device 14 and executing the registration procedure.

More to the point, assuming for the sake of argument that the fingerprint image stored in the memory board is a secure personal database in a single integrated circuit as the Examiner contends (Action at 3), a position Applicant vigorously disputes, Hsu still does not teach or suggest the subject matter defined by claim 15 because it does not teach or suggest "granting said specified user access to said secure personal database [in said single integrated circuit] on biometric verification". To the contrary, Hsu teaches to grant the user access to the memory board containing the stored fingerprint image patches in order to conduct that verification,[2] but is entirely silent on "granting said specified user access to said secure personal database on

[2] This is so because what the Examiner contends is biometric verification in the CRC number generated by access to the memory containing the image patches to compare the scanned fingerprint to the stored image patched.

biometric verification". Rather, as the Examiner interprets Hsu, Hsu teaches away from what is required by Claim 15 by granting the user access to a remote site on biometric verification, e.g., Door 10, and not to a secure personal database an integrated circuit in the portable communications devices.

Alternatively, if as Applicant submits, the Examiner is incorrect in construing the Hsu memory board storing the fingerprint image patches as the secure personal database, then Hsu does not teach or suggest the use of a secure personal database, and also does not teach or suggest granting the user access to it based on biometric verification. In other words, whether or not Hsu teaches biometric verification for opening a remote door, it still does not teach or suggest the subject matter of Claim 15. The Examiner's rejection should therefore be withdrawn.

It should also be noted that Hsu, although employing image-to-image correlation techniques – attempting to match portions of a captured fingerprint image features to the reference image patches stored in memory – does not generate or compare a captured image to a stored *indicia* that represents the algorithmic totality of a fingerprint image (or any other biometric attribute).

Second, Hsu does not teach a multi-function semiconductor device possessing multiple layers of different functionalities combined in a single integrated semiconductor package. The Examiner's assertion to the contrary (Action at 3-4) is the same as saying that a transistor radio circuit is inherently included in a tube-type radio circuit. It is not, as they are different structures, and so, too, the Hsu structure is different than what is called for in Claim 15.

Further, the Examiner asserts Hsu teaches "...If there is a match, the device 14' transmits a confirming message to the door 10, and the door 10 is opened..." [Action at 4.] We

respectfully disagree. According to Hsu, the "confirming message" is the simple binary CRC value that was generated based on the *reference image patches* stored in device 14, not the captioned image. Moreover, the so-called confirming message does not include a biometric (fingerprint) indicia or personal financial information.

Accordingly, because Hsu does not teach or suggest a single integrated circuit that includes a "personal database secure to all but a specified user," and a processor responsive to a biometric sensor and "said secured personal database for verifying the biometric attribute of said specified use, and "granting said specified user access to said secure personal database on biometric verification", as required by Applicant's claim 15, the Examiner's rejection should be withdrawn and claim 15 should be allowed.

Claims 16 and 36

With regard to claim 16, the Examiner alleges that Hsu discloses "means for transmitting ... to a remote location a copy of said sensed biometric attribute in response to a failure to verify said biometric attribute." We respectfully submit that the Examiner is incorrect. The "sensed biometric attribute" is compared to the stored reference image patches – if a match is not confirmed, the CRC generator is not invoked, no CRC binary number is generated, and nothing further happens (see Hsu, figure 3). *There is no transmission as a result of a failure to verify said biometric attribute.* Additionally, the CRC number, if generated, is based on the stored reference image patches and not the sensed biometric attribute. No image, neither the sensed image nor the stored reference image patches, is ever transmitted anywhere. Accordingly, the rejection of Claim 16 should be withdrawn.

With regard to claim 36, the comments above with respect to claim 16 apply equally here. In addition, Applicants note that a simplistic binary CRC value bears no relationship whatsoever to the algorithmic representation of a fingerprint (the biometric attribute) as is contained in an automatic identification indicia. Accordingly, the rejection of Claim 36 should be withdrawn.

For all of the foregoing reasons, withdrawal of the § 102(e) rejection of claims 15, 16, and 36 and the objection to claim 29 based on Hsu is respectfully is requested.

II. Request To Withdraw Final Action

In connection with and prior to filing the RCE application, Applicant sought a first in person interview with the Examiner to discuss this application, which has been pending since October 1999. The Examiner declined to grant that interview, and now has made the first Action on the RCE application Final. As a result, the small entity, independent inventor has been improperly deprived of an opportunity to present arguments to the Examiner, so as to understand better the Examiner's perspective of the prior art and basis for the rejections, and, more particularly, an opportunity to reach agreement on allowable claim language, without being subject to a Final Action. The significance of this is that Applicant has had no meaningful opportunity to amend the claims as a matter of right, if needed, and now is subjected to paying still further fees before having an audience with the Examiner.

Accordingly, Applicant respectfully requests that, if the Examiner determines that this response does not place this application in conditions for allowance, the Examiner withdraw the Finality of the Action, and grant Applicant an interview to discuss and seek agreement on allowable claims and allow applicant an opportunity to amend the claims, if desired, or to

determine whether there is an issue fixed for appeal.

CONCLUSION

Applicant respectfully submits that all of the claims pending in the application now are in condition for allowance. Reconsideration of this application in view of the foregoing remarks respectfully is requested.

The Examiner is invited to call Applicant's undersigned attorney if doing so would expedite prosecution.

The Commissioner is authorized to charge any fee which may be required in connection with this Amendment to deposit account No. 15-0665.

Respectfully submitted,

Dated: 10/16/06

By: _____
Robert A. Isackson, Esq.
Registration No. 31,110

Orrick, Herrington & Sutcliffe LLP
4 Park Plaza, Suite 1600
Irvine, CA 92614-2558
Tel. 212-506-5280
Fax: 212-506-5151
Customer Number: 34313